MULTIMEDIA UNIVERSITY

STUDENT ID NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 2, 2019/2020

TEH3221 – ETHICAL HACKING AND SECURITY ASSESSMENT

(All sections / Groups)

10 MARCH 2020
2.30 p.m – 4.30 p.m
(2 Hours)

INSTRUCTIONS TO STUDENTS

1. This question paper consists of 8 pages, excluding the cover page, with 5 questions only.

2. Attempt **ALL** questions. All questions carry equal marks and the distribution of the marks for each question is given.

3. Please write your answers in the Answer Booklet provided.

Question 1:

Please attempt **ALL** multiple-choice questions. [12 marks]

1. A _____ imitates an attacker and attacks with characteristic tactics and techniques, a _____ is there to find ways to defend, change and re-group defense mechanisms to make incident response much stronger.
   A. red team, blue team
   B. blue team, red team
   C. white team, black team
   D. black team, white team

2. _____ is part of the first phase of a penetration test and allows you to find all network entry points available on a target system.
   A. Networking discovery
   B. Port scanning
   C. Footprinting
   D. Enumeration

3. By consisting only in ASCII characters, _____ strings are generally URL-safe, and that's why they can be used to encode data in Data URLs.
   A. base 2
   B. base 16
   C. base 64
   D. base 8

4. Using _____ against the company's domain allows us to see some of the pertinent information such as who maintains the DNS records and their contact information.
   A. dhclient
   B. dnsquery
   C. nbtscan
   D. whois

Continued .....

5. A(n) _____ is a transceiver that bridges the wireless LAN to wired LAN via an Ethernet cable.
   A. access point (AP)
   B. switch
   C. wireless network interface card (WNIC)
   D. router

6. The ____ command is a powerful enumeration tool included with Windows.
   A. nessusWX
   B. Nbtstat
   C. netDDE
   D. netmon Agent

7. In TKIP enhancements, rekeying mechanism perform which of the following task?
   A. Prevent replays attack
   B. Prevent attackers from injecting forged packets
   C. Prevents attackers from reusing old keys
   D. Create MAC addresses

8. In wardriving, scanning software can identify the followings **except**:
   A. The company's SSID
   B. The type of security enabled
   C. The signal strength
   D. The company's network floor plan

9. _____ causes a system to suddenly stop/ fail when the clock struck 12am of 1 January 2000?
   A. Y2K
   B. Psybot
   C. BIOS-based rootkit
   D. Conficker worm

Continued .....

10. What is the collective name for embedded versions of Windows Enterprise OSs, such as XP Professional, Windows Vista Business and Ultimate, and Windows 7 Ultimate and Professional?
    A. Windows Business Suites
    B. Windows Embedded Enterprise
    C. Embedded Systems Suite
    D. Embedded Windows Servers

11. RC4 in its implementation in _____ has been found to have weak keys. Having a weak key means that there is more correlation between the key and the output than there should be for good security.
    A. WPA
    B. LEAP
    C. WEP
    D. TKIP

12. _____is the first and only publicly accessible cipher approved by the US National Security Agency (NSA) for protecting top secret information. It was first called Rijndael after its two developers, Belgian cryptographers Vincent Rijmen and Joan Daemen.
    A. RC4
    B. DES
    C. DeCSS
    D. AES

Continued .....

Question 2:

a) Fill in the blanks with the most appropriate network attack:

i. _____: a denial-of-service attack caused by an attacker deliberately sending an IP packet larger than the 65,536 bytes allowed by the IP protocol.

ii. _____: a malicious attempt to disrupt normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic from multiple sources.

iii. _____: also known as cookie hijacking is the exploitation of a valid computer session to gain unauthorized access to information or services in a computer system.

iv. _____: a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic.

v. _____: where an individual or organization information is held with ransom. It can be spread to computers through attachments or links in phishing emails, by infected web sites by means of a drive-by download or via infected USB sticks.

[5 marks]

b) Penetration Testing involves a standard approach with different activities to be performed in a sequence. If you are working as a penetration tester, suggest at least **FIVE [5]** mandatory activities to get the project done.

[5 marks]

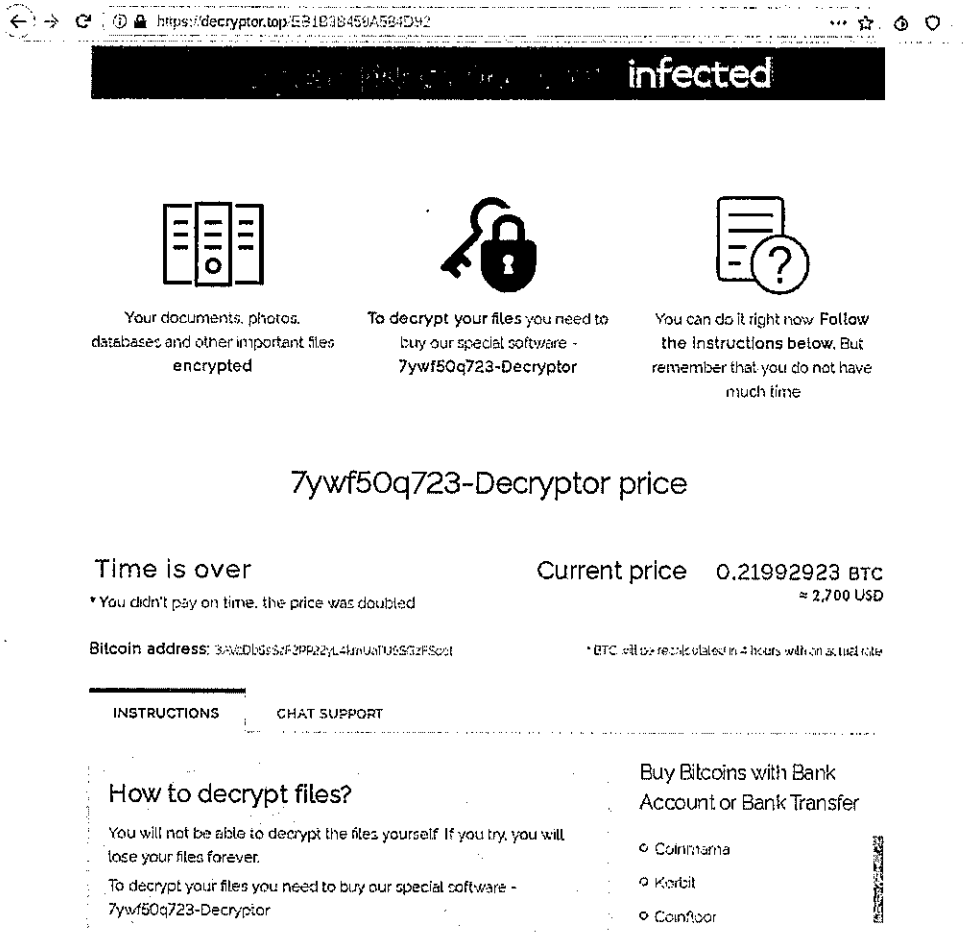
c) Common ports, such as TCP port 80 (HTTP), may be locked down, but other ports may get overlooked and be vulnerable to hackers. When designing your security tests, what are the TCP and UDP ports you should look into? Recommend at least **FOUR [4]** commonly hacked TCP or UDP ports.

[2 marks]

Continued .....

Question 3:

a) If you are seeing this alert, should you pay? Justify your answer and suggest **TWO [2]** countermeasures.


https://decryptor.top/EB1B3B459A584D92
infected
Your documents, photos, databases and other important files encrypted
To decrypt your files you need to buy our special software - 7ywf50q723-Decryptor
You can do it right now. Follow the instructions below. But remember that you do not have much time
7ywf50q723-Decryptor price
Time is over
* You didn't pay on time, the price was doubled
Current price 0.21992923 BTC
≈ 2,700 USD
Bitcoin address:
INSTRUCTIONS
CHAT SUPPORT
How to decrypt files?
You will not be able to decrypt the files yourself. If you try, you will lose your files forever.
To decrypt your files you need to buy our special software - 7ywf50q723-Decryptor
Buy Bitcoins with Bank Account or Bank Transfer
Coinmama
Korbit
Coinfloor

A payment page for a victim of REvil, a.k.a. Sodin and Sodinokibi. Acknowledged to KrebsonSecurity.

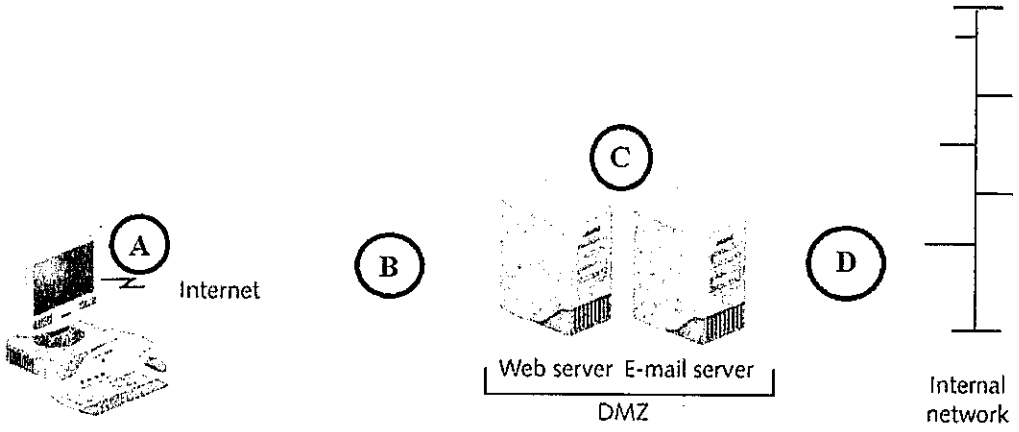
[4 marks]

b) TCP SYN scan is a most popular and default scan in Nmap because it performs quickly compared to other scan types and it is also less likely to block from firewalls. Explain how this scan type works, and how it determines the port status: opened, closed, or filtered.

[5 marks]

Continued .....

c) Referring to the figure below, if you are allocated two firewalls, where will you place them? Explain your answer.



[3 marks]

Continued .....

Question 4:

a) From the `net use` command below, the attack is an infamous vulnerability within Windows, especially to systems prior to XP and Server 2003. It is a connection to a Windows inter-process communication share (IPC$):

```
5
6 C:\>net use \\0.0.0.0\ipc$ "" /user:""
7 The command completed successfully.
```

i. Briefly explain this hacking method.

[2 marks]

ii. Compose **THREE [3]** intentions of this attack.

[3 marks]

iii. Propose **TWO [2]** solutions to overcome this problem.

[2 marks]

b) Explain the following fundamental concepts in programming: **Branching, Looping** and **Testing**.

[3 marks]

c) "*It is not recommended to secure wireless network by using WEP*". Discuss throughout about this statement.

[2 marks]

Continued .....

Question 5:

a) If you managed to establish a NULL connection, what are the information that you can retrieve? Suggest **FOUR [4]** of them.

[4 marks]

b) A hacker enumerated on *ABC Corp.*'s *nix systems with the command of "`finger root`". What are the **FOUR [4]** possible outputs from this enumeration process?

[4 marks]

c) Network Defense department of Multimedia University noticed that a group of attackers is taking control of the university's MMLS server. What are the potential impacts subsequent to this threat? Briefly describe **FOUR [4]** of them.

[4 marks]

End of Page